UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

STATE OF NEW YORK,

Plaintiff,

-v-

CHAD F. WOLF, *in his official capacity as Acting Secretary of Homeland Security*, et al.,

Defendants.

No. 20 Civ. 1127 (JMF)

R. L'HEUREUX LEWIS-MCCOY et al., *on behalf of themselves and all similarly situated individuals*

Plaintiffs,

-v-

CHAD F. WOLF, *in his official capacity as Acting Secretary of Homeland Security*, et al.,

Defendants.

No. 20 Civ. 1142 (JMF)

## DECLARATION

I, Robert E. Perez, hereby state as follows:

1. I am currently the Deputy Commissioner of U.S. Customs and Border Protection (CBP), U.S. Department of Homeland Security. Until November 2018, I was the Executive Assistant Commissioner for Operations Support. I began my career with the U.S. Customs Service in 1992 as a Customs Inspector in Newark, New Jersey. Throughout my career at CBP, I have held various positions at CBP headquarters and in the field, including becoming the first Director of the Customs–Trade Partnership Against Terrorism (C-TPAT) in 2002. I also served as a Port Director and the Director of Field

Operations in Detroit, Michigan, and a Director of Field Operations at CBP's New York Field Office.

2. In my role as Deputy Commissioner, I am the agency's senior career official, with a primary focus of working closely with the Commissioner to ensure that CBP's mission of protecting the Nation's borders from terrorists and terrorist weapons is carried out effectively in partnership with other Federal, state, local, and foreign entities. Additionally, I provide executive leadership in planning short and long-range strategies, activities, and projects.

3. I am familiar with the complaints filed in *State of New York v. Wolf*, Case No. 20-cv-1127 and *Lewis-McCoy v. Wolf*, Case No. 20-cv-1142, filed in the United States District Court for the Southern District of New York and plaintiffs' claims therein.

4. The purpose of this declaration is to explain the impact of the New York Driver's License Access and Privacy Act, also known as the "Green Light" Law, on CBP operations. As a result of the Green Light Law, on December 12, 2019, New York terminated CBP's access to New York Department of Motor Vehicle (DMV) information through the International Justice and Public Safety Network (Nlets). This declaration highlights operational gaps CBP continues to face due to the Green Light Law in its newly amended form, including difficulties that CBP would have in adhering to New York's law, as amended, if data access were to be restored.

5. This declaration is based on my personal knowledge, as well as information conveyed to me by my staff and other knowledgeable CBP personnel in the course of my official duties and responsibilities.

### A. Impact of the Amendment to the Green Light Law

6. On April 3, 2020, New York enacted the Fiscal Year 2020-2021 Budget, which amended the "Green Light" Law to permit the sharing of DMV information with CBP for vetting Trusted Traveler Program (TTP) applicants and vehicle importation and exportation purposes. N.Y. Veh. & Traf. Law § 201.12(a) (as amended April 2020) (hereinafter "the Amendment"). However, despite this Amendment, CBP access to NY DMV data through Nlets for purposes of TTP vetting (or for any other purpose) has not yet been restored. Accordingly, as of the date of this declaration, CBP cannot vet TTP applicants from the State of New York to determine their eligibility for TTPs.

7. While the Amendment to the Green Light Law appears to carve out an exception for TTP vetting from the law's general prohibition on providing New York DMV information to any agency that primarily enforces immigration law, it also makes it a class E felony to use DMV information for immigration purposes. This addition of potential criminal liability presents risks of personal liability for CBP employees as well as state and local partners interacting with CBP.

8. Were CBP to gain access to New York DMV data for TTP vetting purposes, the Amendment would nonetheless restrict CBP's ability to disseminate the DMV data obtained for TTP vetting purposes within its databases or amongst its staff for purposes necessary to carry out CBP's mission. Such restriction on the use of DMV data would have a negative impact on CBP operations by creating gaps in the universe of information CBP relies on to carry out its critical mission and posing significant officer safety concerns. Officers conducting their respective duties may manually share information necessary to fulfilling their responsibilities. The Amendment presents CBP

officers with a choice of either following NY law or properly fulfilling their statutory mandates.

9. CBP has a broad mission to protect the Homeland from dangerous people and cargo and to prevent terrorists and terrorist weapons from entering the United States, while facilitating legitimate trade and travel. To carry out its broad mission, CBP engages in a variety of activities ranging from the interdiction of counterfeit goods and human trafficking operations to the prevention of terrorists and weapons of mass destruction from entering the United States. These diverse functions often overlap as officers respond to information uncovered during inspections or investigations. Access to, and the fluid flow of, current information and the ability to cross-reference information across multiple databases serve as the foundation of CBP's critical law enforcement function.

10. Because of the way CBP systems and operations are designed, information obtained for TTP purposes may in certain circumstances be entered across multiple law enforcement databases. For example, this information may be used to further CBP's law enforcement mission of inspecting all persons arriving to the United States to determine citizenship and admissibility under the immigration laws, as appropriate. As such, while the Amendment allows for use of DMV information for TTP vetting purposes only, adherence to the Amendment's restrictions on the downstream use of that information would create gaps in other critical areas of CBP's congressionally mandated mission.

11. As discussed above, access to DMV information is facilitated through Nlets. CBP has separate Originating Agency Identifiers (ORIs) specific to its mission responsibilities, including one for TTP vetting. CBP employees whose duties include these activities are

authorized access to make queries related to their mission responsibilities via Nlets. The Nlets queries are automatically run via the vetting system and reviewed by authorized CBP officers. CBP officers conducting TTP vetting review the DMV data and may run additional queries through Nlets to refine these results. Relevant information is then entered on a risk assessment worksheet that is transmitted to CBP's Global Enrollment System (GES) that houses TTP membership records. The risk assessment worksheet could include information that is a basis for a denial of TTP membership and/or potentially derogatory information that needs to be addressed by an enrollment center officer during an interview in order to determine whether or not the applicant is eligible for TTP membership. The risk assessment worksheet with any pertinent DMV information is then entered into and stored in GES. GES is accessible to a certain set of individuals within CBP who have a "need-to-know" for the information housed therein for vetting and investigative purposes. Records related to TTP decisions must be retained for accountability purposes.

12. CBP personnel who do not have routine access to New York DMV data through Nlets for TTP vetting could access such information if the information is manually recorded in other CBP systems. In addition, DMV information obtained for TTP vetting purposes could be shared on an ad hoc and "need-to-know" basis among CBP officers and between CBP and other authorities if such information is relevant to an ongoing investigation. During TTP vetting, information from DMV records may be incorporated into risk assessments or input into TECS[1] (e.g., in connection with the creation of a lookout

[1] TECS (not an acronym) is CBP's principal law enforcement system that houses temporary and permanent enforcement, inspection, and intelligence records relevant to the law enforcement mission of CBP and numerous other federal agencies that it supports. TECS is described in further detail in the Federal Register at 73 Fed. Reg. 77778 (Dec. 19, 2008).

record), as appropriate. If that occurs, other individuals within CBP who have authorized access to TECS (or other government agencies that have access to such information in TECS pursuant to an information sharing agreement) would have access to that information and could potentially use it for immigration enforcement purposes, in addition to other law enforcement and homeland security purposes.

13. In addition to TECS, DMV information may also be accessible in other law enforcement systems that CBP uses to identify individuals and cargo that may require additional scrutiny during inspection. CBP's Automated Targeted System (ATS)[2] compares information on travelers and cargo arriving in, transiting through, and exiting the country against information from law enforcement and intelligence databases. In addition, ATS allows appropriately provisioned users to conduct queries across multiple databases, including TECS, GES, Nlets, and others, to provide a consolidated view of data responsive to all underlying queries about a person or entity. If DMV information obtained during vetting of a TTP applicant were to be recorded in TECS or GES, such information could potentially be viewed in ATS by CBP officers assessing whether certain travelers or cargo require additional scrutiny. Access to ATS is limited to those individuals who have a "need-to-know" and are authorized such access in order to carry out their official duties. Furthermore, access to specific data sets within ATS is further controlled by providing each user only those accesses required to perform his or her job.

[2] DHS/CBP/PIA-006 Automated Targeting System, September 2014, https://www.dhs.gov/publication/automated-targeting-system-ats-update.

14. The DMV information that is recorded in other CBP systems is retained according to the data retention schedules applicable to those law enforcement systems and published in Privacy Act notices.[3]

15. The ability to view and connect data across multiple databases and systems is a critical component of CBP's ability to make necessary connections between pieces of information in order to both effectively assess the risk of individuals and cargo seeking to enter or depart from the United States and to properly police between ports of entry. Even if CBP were to receive New York DMV information for use in TTP vetting, in order to shield CBP employees from potential criminal liability, the Amendment would require CBP to silo that information from its databases, preventing law enforcement officers who may be conducting critical investigations, including those related to terrorism, from identifying connections between individuals or relevant information.

16. The National Commission on Terrorist Attacks Upon the United States (9-11 Commission) determined that hindsight review of previous tragedies indicates that information sharing and cooperative action are integral to identifying and resolving threats before they occur. In accordance with the 9-11 Commission's findings and recommendations, CBP systems were developed to promote the efficient and effective flow of information to best promote border and national security, avoiding the segregation of information that impeded law enforcement in the past. In developing these systems, CBP also incorporated rigorous data security and privacy protections to ensure the proper handling of all data in its custody. New York's Green Light Law

[3] DHS/CBP/PIA-021, TECS System: CBP Primary and Secondary Processing (August 12, 2016), available at www.dhs.gov/privacy; DHS/CBP/PIA-009(a) TECS System: CBP Primary and Secondary Processing (TECS) National SAR Initiative (August 5, 2011), available at www.dhs.gov/privacy; DHS/CBP-011; DHS/CBP-011 TECS, System of Records, 73 Fed. Reg. 77778, 77782 (Dec. 19, 2018).

would require CBP to reverse decades of efforts to achieve the fluid network of information sharing across the government that was deemed critical by the 9-11 Commission to avoid future threats to our nation's security. The importance of unimpeded information sharing was demonstrated in 2010 when state and local data accessed by CBP proved critical in leading to the capture of the New York City Times Square bomber as he was about to depart the country. In a more recent example, when federal authorities responded to the scene of the 2017 Halloween attack in New York City, they contacted CBP to verify the identity of the attacker using his recovered driver's license and obtain other critical information regarding the subject. The very first step CBP took was to query Nlets to determine whether the suspect's identity on his driver's license was authentic before conducting queries in other law enforcement systems to assist law enforcement with the investigation.

17. Not only would New York law require CBP to alter its systems, but its policies and culture would also need to be drastically changed, in direct contravention of the 9-11 Commission's findings and recommendations, to create partitions between CBP operational offices and DHS components as well as between CBP and its inter-agency partners. The imposition of artificial barriers to information flow would harmfully impede CBP's ability to carry out its mission of protecting the Homeland from dangerous people and cargo and simultaneously deprive other U.S. government authorities of information that may be critical to significant criminal and terrorism investigations.

### B. CBP's Use of DMV Information Outside of TTP Vetting

18. CBP utilizes DMV data throughout its operations, and access greatly facilitates the efficiency of operations, the allocation of resources to properly reflect potential threat,

and the promotion of officer and public safety. DMV data allows officers access to information that can ensure the validity of individuals' identities and documents in areas such as vetting, inspection, and general law enforcement operations. For example, at ports of entry (POEs), access to DMV data (via license plate readers and manual searches) allows inspecting officers to verify ownership of vehicles being used to cross the border, as well as the validity of documents presented to the officer. DMV data conveys critical information to the officer that could signal a need for further inspection or prompt safety precautions. During secondary inspection, officers may query DMV information to gain a more holistic view of an individual and come across information such as criminal activity or a suspended license that could potentially warrant local/state law enforcement intervention to ensure public safety. Border Patrol Agents utilize DMV information to better understand who they may be approaching during traffic stops and may use DMV information to connect cars utilized in illicit activity to owners and addresses that are associated with important national security concerns and other law enforcement matters, such as human smuggling and illicit drug trafficking. Further, identifying information in the DMV, such as an individual's address, may be essential to a wide range of purposes, from locating witnesses to ensuring that CBP is hiring individuals who are suitable for employment. Being able to fluidly share information with other government partners is integral to the nation's security and to ensuring that law enforcement is best equipped to address situations as they transpire.

19. Lack of access to New York's DMV data creates blind spots in CBP's understanding of its operational environment, such that officers and the public are unnecessarily put at risk. The New York law also impacts CBP's ability to effectively conduct risk

assessments of persons and cargo crossing the border, a purpose aimed at ensuring the enforcement of U.S. laws generally, which include the immigration laws. It also impacts CBP's ability to interdict subjects who may be engaged in criminal activities between the ports of entry. Finally, in rural areas, such as upstate New York, CBP will oftentimes assist state and local partners and will be the first agents on scene for numerous dangerous incidents. In such circumstances, the ability to query Nlets often is most crucial to determine the identity of suspects.

20. Without full access to New York DMV data for all areas of CBP's mission, critical connections will be missed, which could lead to grave consequences.

I declare that the foregoing is true and correct to the best of my knowledge, information, and belief.

Executed on the 17TH day of June, 2020

/s/
Robert E. Perez
Deputy Commissioner
U.S. Customs and Border Protection